



Experimental validation of GNSS repeater detection based on antenna arrays for maritime applications

Manuel Appel^{1,2} · Andreas Iliopoulos¹ · Friederike Fohlmeister^{1,3} · Emilio Pérez Marcos¹ · Manuel Cuntz^{1,2} · Andriy Konovaltsev¹ · Felix Antreich^{1,4} · Michael Meurer^{1,2}

Received: 31 March 2017 / Revised: 11 December 2018 / Accepted: 17 December 2018 / Published online: 28 December 2018
© The Author(s) 2018

Abstract

In this work, we present an antenna array-based algorithm to detect GNSS repeater and/or spoofing attacks with an experimental validation. With an array receiver capable of measuring the impinging ranging signals direction of arrival in terms of azimuth and elevation, it is possible to estimate the antenna platforms attitude. The fact that this information is computed (w.r.t. a reference frame) during the position calculation is used. We propose an algorithm aiming to find the relation between both representations. This mapping defines the receiver's attitude in terms of pitch, roll and yaw angle. The residual of this mapping is used to construct a quality metric for the mapping. If a threshold is undershot, spoofing/repeating is indicated. The performance is demonstrated using software simulations. To show the capabilities under realistic conditions, a test platform is described. It consists of a real-time array receiver and a sampling device enabling post-processing. A maritime measurement campaign including two vessels—one acting as receiver and the other acting as transmitter—is portrayed. Finally, the real-time and post-processing performance of the algorithm is evaluated.

Keywords Global navigation satellite systems (GNSS) · Maritime navigation · Repeater detection · Spoofing detection · Attitude estimation · Antenna array signal processing

1 Introduction

Nowadays, global navigation satellite systems (GNSS) are an essential part of many systems in the maritime community. The position information provided by the GNSS receivers is usually fused with other sensors like inertial measurement units (IMUs) or magnetic gyroscopes. The subsystem of sensors is subsequently integrated with electronic navigation charts (ENCs) and/or the automatic identification system (AIS), which is mandatory for larger vessels. This way,

the main positioning, navigation and timing (PNT) unit—required for ships of a certain class—is formed.

The majority of accidents in the maritime context are caused by human error. Recent studies [1, 2] exploited that fact. A prominent example for a recent incident, which caused heavy public attention, is the Costa Concordia accident [3]. Misuse of the ship's navigation system by the captain was discovered to be the reason. The introduction of autonomous and trustworthy semi-autonomous systems can very likely prevent such catastrophic events in future. Getting towards reliable systems, the International Maritime Organization (IMO) specifies and promotes the “e-Navigation” concept [4]. The goal is to achieve an integration of already existing electronic navigation devices.

One key element to implement the “e-Navigation” concept is to get towards a standardization of GNSS receivers' positioning performance requirements in terms of integrity, accuracy and availability. Current activities aim to terrestrial (differential GNSS) or satellite-based (SBAS) augmentation systems in order to match the positioning requirements given by different (non-global) standards.

✉ Manuel Appel
manuel.appel@dlr.de

¹ German Aerospace Center (DLR), Inst. for Communications and Navigation, Oberpfaffenhofen, Germany

² Chair of Navigation, RWTH Aachen University, Aachen, Germany

³ Technical University of Munich (TUM), Munich, Germany

⁴ Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos, SP, Brazil

Studies [5] have been carried out to show the vulnerability of GNSS signals in maritime environments. Several sea trials have been performed by the General Lighthouse Authorities of the United Kingdom and Ireland (GLA) in collaboration with the UK Ministry of Defense (MOD). These studies aimed at exploiting the effects of jamming (i.e. radio frequency interference) on security and safety of maritime navigation [6]. An important result of the trials is that not only the positioning system is affected by interference. Since the positioning is an essential input for many different subsystems, many safety-critical applications (i.e., digital situation awareness, chart stabilization, digital selective calling and emergency communication) are affected as well.

For several decades, many research groups as well as receiver manufacturers have taken efforts to detect and mitigate RF interference. Due to the large traveling distance (more than 20,000 km) of the electromagnetic wave emitted by the navigation satellites towards the surface of the earth, a receiver is vulnerable to even unintentional interference. Since the transmission power of the satellites is in the order of 50 W the received power drops down to some femtowatts. This increases the risk for operational outages or performance degradation [7]. Systems sharing the same frequency band [e.g., aviation Distance Measurement Equipment (DME) for Galileo E5a] or systems operating in different bands but emitting harmonics in the GNSS bands [user terminals for mobile satellite systems (MSS)] are examples for unintentional interferers.

In contrast to that, intentional interference becomes a major issue not only in a military context. This is due to the almost unlimited availability of (cheap) so-called personal privacy devices (PPDs). By transmitting a relatively high-power signal, GNSS receivers (used for critical infrastructures) in a wide range are affected and therefore cannot deliver positioning (and timing) information anymore [8].

In the light of that, large maritime organizations, such as the Lloyd's [9] register but also the European Global Navigation Satellite Systems Agency (GSA) [10], foresee that the field of navigation robustness and cybersecurity will be a major challenge and trend for the maritime community in the upcoming years.

Operational outages or performance degradation is of minor concern, if they are detected. This can be achieved by constantly monitoring the relevant spectrum and declare the system unhealthy if a radio frequency interference (RFI) event was identified.

However, during the last decade a different type of threat gained much attention in the GNSS community: the so-called “spoofing” threat. The ultimate goal of a spoofer is not to block but to control a victims receiver's position (and time) measurement without being detected. The threat is not only of academic interest, but has also been demonstrated

in reality. Especially in the maritime context, the authors of Ref. [11] have shown the vulnerability of a ship's navigation system by spoofing a luxury yacht. Using the same self-developed spoofer [12], the research group could demonstrate, that also unmanned aerial vehicles (UAVs) [13] and critical infrastructures, such as power grids [14], are vulnerable against spoofing. In addition, several experiments performed under laboratory conditions [15] using signal generators generating different types of spoofing attacks showed the vulnerability of professional aeronautical receivers. Subcategories of the threat are so-called repeating (unintentional re-radiation) and meaconing (intentional re-radiation). The similarity to spoofing is the presence of GNSS-like signals at a “victim” receiver's antenna.

If successful and undetected, the attack may cause major damage—not only in a monetary sense, but also to lives. Several possible receiver autonomous detection schemes have been presented in the literature. For single antenna receivers, the detection relies on the behavior of different signal parameters which are estimated during regular operation. Examples are signal power, Doppler frequency offset, the PRN code delay and its rates, the shape of the correlation function as well as the relation of the signal components at different carrier frequencies (see [16, 17] and [18] for instance). However, the most advanced protection against sophisticated spoofing attacks can be provided by using antenna arrays and utilizing signal processing in the spatial domain [19–24]. A GNSS receiver with multiple antennas is able to estimate the directions of arrival (DoA) of the impinging waveforms and therefore to distinguish between the authentic and counterfeit signals.

The remainder of the paper is organized as follows: first a system description is introduced, which leads to a mathematical description of the attitude estimation problem. Based on that derivation, a metric for anomaly detection is deduced. Combining these two results, an algorithm for joint attitude estimation and spoofing/repeater detection is presented. In the next chapter, a description of the test platform (including the array) is provided. Subsequently, the experimental evaluation as well as the results are presented. Finally, a summary and conclusion is provided.

2 Notation

The following notation is used throughout the paper:

- \mathbf{x} : Bold face lower case letters denote column vectors.
- \mathbf{X} : Bold face capital letters denote matrices.
- \mathcal{X} : Calligraphic letters denote sets.
- $|\mathcal{X}|$: The number of elements contained in a set (cardinality).

- $(\cdot)^T$: The transpose of a vector or matrix.
- $\text{tr}(\cdot)$: The trace (i.e. sum of all diagonal elements) of a matrix.
- $\text{diag}(\mathbf{x})$: Creates a quadratic matrix, with the vector \mathbf{x} on its main diagonal. All other entries are zero.

3 System description

The goal of the architecture is to estimate the attitude of an antenna array-based receiver platform w.r.t. an east–north–up reference coordinate frame. To make the work at hand as self-contained as possible, the analysis performed in [22] or [25]¹ and later used in Ref. [27] are revisited. The corresponding estimation problem as well as a way to solve it is presented. The derivation provides deeper insights and naturally leads to a detection scheme.

The system's core is an antenna array-based GNSS receiver. Assuming enough degrees of freedom (i.e. antennas), a measurement of the ranging signal's elevation and azimuth is performed in the post-correlation domain, by using, for example Unitary ESPRIT [28] (if the geometry and pattern are sufficient to fulfill the assumptions). The message decoding and position calculation (PVT) is assumed to be available. Figure 1 depicts a block diagram of the generic system setup.

$s_1(1) \dots s_L(n)$ denote the sampled baseband representation of the input signals received by the L elements of the array antenna. By measuring the DoA of the incoming ranging signals, directional cosines² pointing from the origin of the antenna's local reference frame towards the source (i.e. the satellites) are available. These are denoted by $\mathbf{b}_j \in \mathbb{R}^3$ and collected in the set $\mathcal{B} = \{\mathbf{b}_j\}_{j \in J}$. They are represented in a local antenna coordinate system (details can be found in Ref. [21]). J denotes the set of the corresponding PRN numbers of satellites with available measurements.

Decoding the almanac information allows calculation of direction cosines in an east–north–up (ENU) coordinate frame. The set is denoted by $\mathcal{A} = \{\mathbf{a}_i\}_{i \in I}$. I denotes the set of PRN numbers, which are evaluated by the receiver. If it is assumed that the almanac information is available for all tracked satellites J is a subset of I .

Both coordinate frames are rotated versions of each other. The following equation for all pairs $K = J \cap I$ of available measurements and references can be stated:

$$\mathbf{b}_k = \mathbf{R} \mathbf{a}_k \quad \forall k \in \mathcal{K}. \quad (1)$$

¹ Recently also published in [26, Chapter 27], both are using slightly different terminologies.

² Unit vectors.

³ See [29], $\mathcal{SO}(n) = \{X \in \mathbb{R}^{n \times n} | XX^T = \mathbf{I} \wedge \det(X) = 1\}$

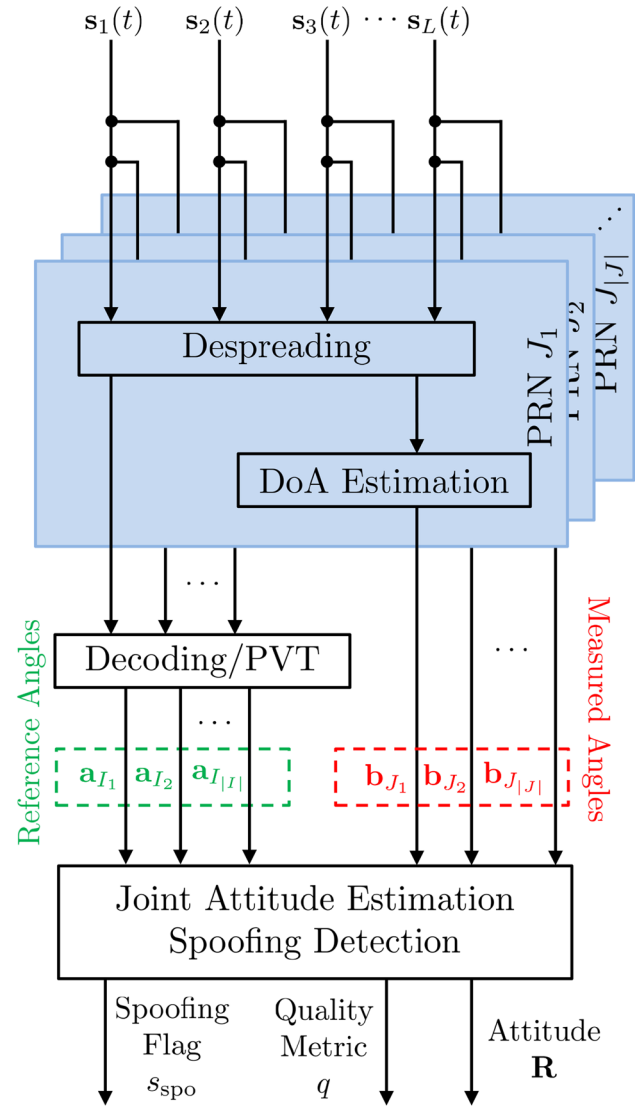


Fig. 1 Block diagram of the generic system setup (taken from [22])

The rotation is represented by a rotation matrix $\mathbf{R} \in \mathcal{SO}(3)$ ³ (special orthogonal group). It contains the information about roll, pitch and yaw angle and therefore defines the current attitude. This rotation (i.e. attitude) describes the rotation of the ENU into the antenna coordinate frame at certain time instant when the PVT and DOA estimates are available. It therefore is a property of the receiver platform.

3.1 Measurement model

The ephemeris and PVT-based directional cosines $\{\mathbf{a}_i\}_{i \in I}$ are assumed to be perfectly known. This is justified by the large distance between the satellites and the surface of the earth (more than 20,000 km), where the receiver is expected to be. However, the array-based estimates suffer

from imperfections. In Ref. [21] these errors are modeled using additive Gaussian noise ($\mathbf{n}_k \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{I})$), yielding:

$$\mathbf{b}_k = \mathbf{R}\mathbf{a}_k + \mathbf{n}_k \quad \forall k \in \mathcal{K}. \quad (2)$$

It should be mentioned, that if the corresponding vectors \mathbf{a}_k and \mathbf{b}_k are unit vectors and both are rotated versions of each other, in a strict sense Eq. (2), cannot hold without further restrictions on the noise.

It seems convenient to model these errors using rotation matrices as well, since the noise affects the orientation of the directional cosines:

$$\mathbf{b}_k = \mathbf{R}_k \underbrace{\mathbf{R}\mathbf{a}_k}_{\mathbf{b}_k^{\text{perf}}} \quad \forall k \in \mathcal{K}. \quad (3)$$

A construction of these matrices can be performed by choosing a random rotation axis $\boldsymbol{\omega}_k$ and a random angle α_k for each measurement separately.

3.2 Snapshot-based problem statement

The ultimate goal of the algorithms that we are developing in this work is to perform a computation of the rotation matrix \mathbf{R} (which corresponds to the current attitude) and to detect anomalies in the DoA measurements (which could be caused by “spoofing” or meaconing).

Using the noise model described in Eq. (3), the following set of equations for $N = |\mathcal{K}|$ different pairs of measurements can be stated:

$$\begin{aligned} \mathbf{b}_1 &= \mathbf{R}_1 \mathbf{R} \mathbf{a}_1 \\ &\vdots \\ \mathbf{b}_k &= \mathbf{R}_k \mathbf{R} \mathbf{a}_k \\ &\vdots \\ \mathbf{b}_N &= \mathbf{R}_N \mathbf{R} \mathbf{a}_N. \end{aligned} \quad (4)$$

In the following, $\mathbf{B} \in \mathbb{R}^{3 \times N}$ and $\mathbf{A} \in \mathbb{R}^{3 \times N}$ denote matrices consisting of the available DoAs in their columns. Following the maximum likelihood principle, one is interested to minimize the noise of the measurement rotation. Therefore, the distance of the noisy versions of \mathbf{b} [see Eq. (3)] and the unaffected ones $\mathbf{b}_k^{\text{perf}}$ is to be minimized.

Since the noisy rotations are assumed to be independent for different unit vectors, a measure $g(\cdot)$ for this distance is employed for each unit vector. The results are summed up, yielding the following cost function for the antennas’ attitude:

$$f(\mathbf{R}) = \sum_{k=1}^N \underbrace{g(\mathbf{R}\mathbf{a}_k - \mathbf{b}_k)}_{\text{Difference caused by noise}}. \quad (5)$$

Using the squared ℓ_2 -norm for $g(\cdot)$ the following ML-based optimization problem can be stated:

$$\mathbf{R}^* = \arg \min_{\mathbf{R} \in \mathcal{SO}(3)} \|\mathbf{R}\mathbf{A} - \mathbf{B}\|^2. \quad (6)$$

Other possible choices for $g(\cdot)$ can be found in Ref. [29] by constructing the induced norms from the metrics described therein. This optimization problem (which was derived in this work) is also known as Wahba’s problem (see for instance [30]).

3.3 Closed-form solution

In Ref. [21] an iterative approach was used to solve the problem stated in Eq. (6). In the following section a closed-form solution is derived, allowing further insight in the geometric properties and conditioning (i.e. under which conditions a solution exists) of the problem.

The side condition $\mathbf{R} \in \mathcal{SO}(3)$ is a more special case of $\mathbf{R} \in \mathcal{O}(3)$ ⁴, as $\mathcal{SO}(n) \subset \mathcal{O}(n)$ (i.e. mirroring is allowed for the orthogonal group). This implies six equality constraints, due to symmetry. Defining $\mathbf{S} = \mathbf{R}\mathbf{R}^T \in \text{Sym}(3)$ ⁵, these read:

$$s_{k,k} = 1 \quad \forall \quad 1 \leq k \leq 3, \quad (7)$$

$$s_{k,l} = 0 \quad \forall \quad 1 \leq k < l \leq 3, \quad (8)$$

$$s_{k,l} = 0 \quad \forall \quad 1 \leq l < k \leq 3. \quad (9)$$

Equations (8) and (9) are redundant since $s_{k,l} = s_{l,k}$. For the optimization, this yields six equality constraints. A matrix $\boldsymbol{\Lambda} \in \text{Sym}(3)$ is used to collect the Lagrangian multipliers. By constructing a function $h(\cdot)$ [see Eq. (10)], all six equality constraints are summed up. Setting this sum to zero is a more relaxed but still necessary condition compared to stating them separately:

$$h(\mathbf{R}) := \text{tr}(\boldsymbol{\Lambda}(\mathbf{R}\mathbf{R}^T - \mathbf{I})) = 0. \quad (10)$$

The Lagrangian cost function therefore reads:

$$L(\mathbf{R}, \boldsymbol{\Lambda}) = \|\mathbf{R}\mathbf{A} - \mathbf{B}\|^2 + \text{tr}(\boldsymbol{\Lambda}(\mathbf{R}\mathbf{R}^T - \mathbf{I})). \quad (11)$$

The standard approach (see [31] for instance) is performed by setting the gradient w.r.t \mathbf{R} to zero and we get:

$$\frac{1}{2} \nabla_{\mathbf{R}} L(\mathbf{R}, \boldsymbol{\Lambda}) = \mathbf{R}(\mathbf{A}\mathbf{A}^T + \boldsymbol{\Lambda}) - \mathbf{B}\mathbf{A}^T = \mathbf{0}, \quad (12)$$

$$\underbrace{\mathbf{R}(\mathbf{A}\mathbf{A}^T + \boldsymbol{\Lambda})}_{\text{lhs}} = \underbrace{\mathbf{B}\mathbf{A}^T}_{:= \mathbf{C} = \text{rhs}}. \quad (13)$$

⁴ $\mathcal{O}(n) = \{\mathbf{X} \in \mathbb{R}^{n \times n} | \mathbf{X}^T \mathbf{X} = \mathbf{I}\}$.

⁵ Symmetric, quadratic matrices: $\text{Sym}(n) = \{\mathbf{X} \in \mathbb{R}^{n \times n} | \mathbf{X} = \mathbf{X}^T\}$.

The side condition (\mathbf{R} to be orthogonal) can be used in a tricky way to solve for $\mathbf{\Lambda}$. The transpose of the right-hand side (rhs) of the above equation is multiplied from the left. The term containing \mathbf{R} cancels out. The remaining term in brackets is symmetric (due to the redundancy in $\mathbf{\Lambda}$). The result reads:

$$(\mathbf{A}\mathbf{A}^T + \mathbf{\Lambda}) = (\mathbf{C}^T \mathbf{C})^{\frac{1}{2}}. \quad (14)$$

Combining this result with Eq. (13) yields:

$$\mathbf{R}(\mathbf{C}^T \mathbf{C})^{\frac{1}{2}} = \mathbf{C}. \quad (15)$$

Using a singular value decomposition for $\mathbf{C} := \mathbf{U}\mathbf{\Sigma}\mathbf{V}^T$, the result can be further simplified. Due to the properties of $\mathbf{U} \in \mathcal{O}(3)$ and $\mathbf{V} \in \mathcal{O}(3)$ the following result can be stated:

$$\mathbf{R}\mathbf{V}\mathbf{\Sigma} = \mathbf{U}\mathbf{\Sigma}. \quad (16)$$

To finally solve for \mathbf{R} , the matrix $\mathbf{\Sigma} = \text{diag}(\sigma_1, \sigma_2, \sigma_3)$ has to be further investigated. Without loss of generality, the singular values are ordered decreasingly. Three cases can be distinguished, since if at least one measurement is available, the minimum rank of \mathbf{C} is one.

1. All singular values are unequal to 0:

$\mathbf{\Sigma}$ is invertible. The result for \mathbf{R} reads:

$$\mathbf{R}' = \mathbf{U}\mathbf{V}^T. \quad (17)$$

To ensure that a proper rotation matrix (the constraint $\det(\mathbf{R}) = 1$ was not taken into account so far) is derived, the following “normalization” has to be performed:

$$\mathbf{R} = \mathbf{U} \text{diag}(1, 1, \det(\mathbf{U}\mathbf{V}^T)) \mathbf{V}^T. \quad (18)$$

2. One singular value is equal to 0:

This corresponds to the case, where the set of $\{\mathbf{a}_k\}_{k=1}^N$ or $\{\mathbf{b}_k\}_{k=1}^N$ span only two dimensions. Since the goal of the optimization is to rotate one coordinate system onto the other, this information is enough, since the missing one is uniquely determined. The result for \mathbf{R} therefore is the same as in the previous case.

3. Two singular values are equal to 0:

This case occurs, if only one direction is present in either $\{\mathbf{a}_k\}_{k=1}^N$ or $\{\mathbf{b}_k\}_{k=1}^N$. If more than one measurement is available, this is very unlikely for a GNSS constellation (almanac data). If the measurements however span only one dimension, an anomaly is very likely, which makes an attitude determination impossible.

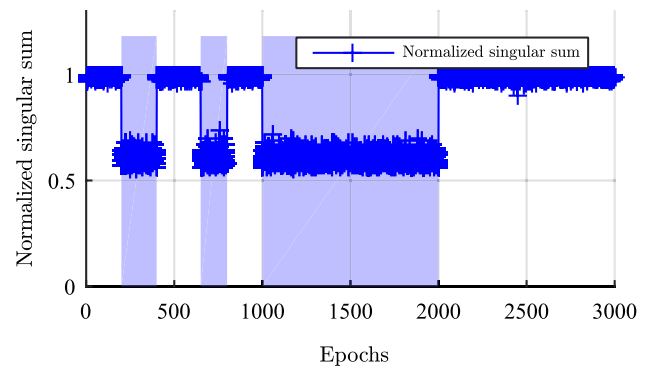


Fig. 2 Sum of singular value-based detection of anomalies with noisy measurements (noise variance is 10 degree²)

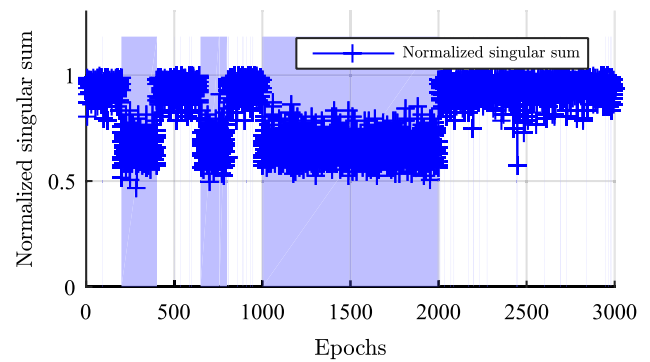


Fig. 3 Sum of singular value-based detection of anomalies with noisy measurements (noise variance is 25 degree²)

4 Anomaly detection

As already mentioned in the previous section, an inspection of the singular values of $\mathbf{C} = \mathbf{B}\mathbf{A}^T$ can be used to detect anomalies. Computing the sum of singular values as a metric is discussed in this section.

By definition, directional cosines have length one. This implies, that the sum of all singular values (of \mathbf{C}^6) is equal to $N = |\mathbf{K}| = |\mathbf{I} \cap \mathbf{J}|$. This property is used for inspection.

For noisy measurements, the normalized (divided by N) sum can be computed, yielding values in the interval $[0, 1]$. If the resulting metric is below a certain threshold ϵ an anomaly is very likely. Figure 2 shows an example with moderate noise based on computer simulations. For all simulations, a fixed but randomly chosen constellation⁷ has been generated. The approach works for that case. A blue background depicts the presence of a repeater for the simulation. A raised flag indicates the detection.

⁶ For perfect (i.e., noiseless) measurements.

⁷ All satellites in view are above the receiver, i.e., their z -coordinate w.r.t. the ENU-frame centered around the receiver is positive.

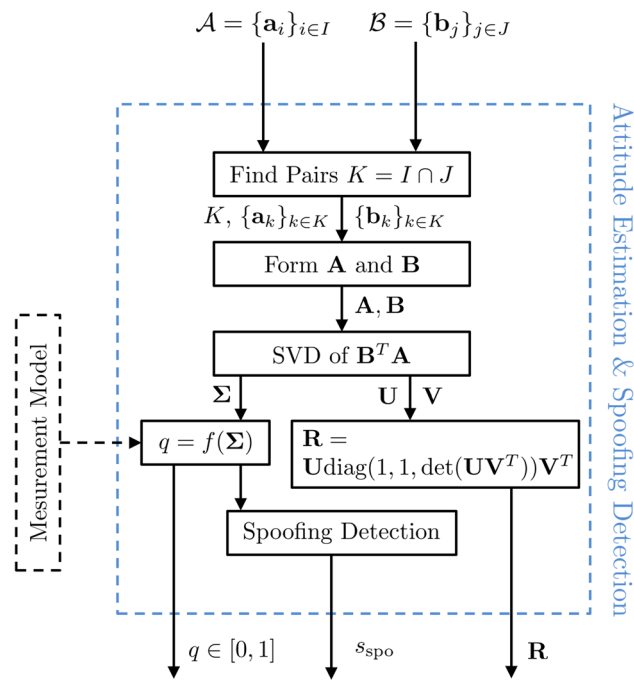


Fig. 4 Block diagram of the basic snapshot-based algorithm (taken from [22])

The results for more noisy measurements (a variance of 25 degree²) is shown in Fig. 3. A reliable detection cannot be performed in that case, i.e., no threshold can be found to yield an acceptable misdetection and false alarm rate. The spoofer was turned on for the same time instances as in the previous simulation (indicated by the blue background again). The detection-flag is indicated in blue. It should be mentioned that the statistic not only depends on noise, but also on the current geometry, i.e. the satellite constellation and the direction of the spoofer/repeater.

5 Snapshot-based attitude estimation

To summarize the results derived so far, the block diagram of the basic snapshot-based algorithm (depicted in Fig. 4) is presented. A quality metric based on the normalized sum of singular values $q \in [0, 1]$ is computed by the algorithm:

$$q = f(\Sigma) = \frac{1}{N} \sum_{k=1}^3 \sigma_k. \quad (19)$$

A flag indicating spoofing s_{spo} by comparing the sum with a certain threshold ϵ is returned as well:

$$s_{\text{spo}} = \begin{cases} 1 & : 0 \leq q \leq \epsilon \\ 0 & : \epsilon < q \leq 1. \end{cases} \quad (20)$$

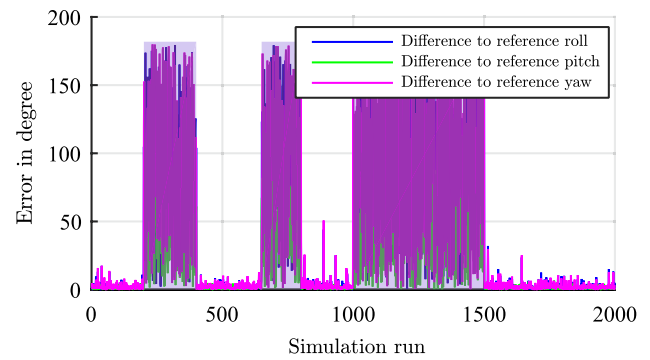


Fig. 5 Difference to reference for roll, pitch and yaw in degree; the noise variance was 5 degree² and $N = 6$

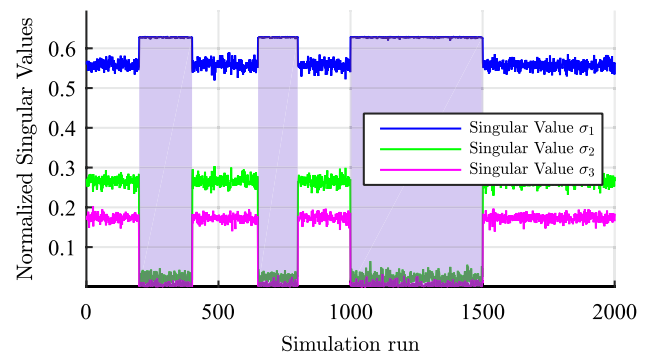


Fig. 6 Normalized singular values of C ; the noise variance was 5 degree² and $N = 6$

First, the performance is analyzed using simulated data sets. A random almanac consisting of N unit vectors is generated. Afterwards a random attitude is generated by choosing a unit vector for the rotation axis and a scalar rotation angle randomly. The almanac unit vectors are then rotated by this attitude, yielding $\{\mathbf{b}_k^{\text{perf}}\}_{k=1}^N$. Finally, the measurements are generated by again generating a random rotation (with the constraint, that the rotation axis is orthogonal to \mathbf{b}_k).

Optionally a spoofer can be turned on for specified simulation runs. This will force all DoA estimates of the impinging signals to have the same azimuth and elevation, before noise is added. For the described examples, the affected simulations are the ones in the intervals [200, 400], [650, 800] and [1000, 1500].

5.1 Example 1: low noise with six signals

Figure 5 shows some exemplary results for 2000 subsequent runs using a noise variance of 5 degree² and 6 reference angles. Figure 5 shows the same setup for only three

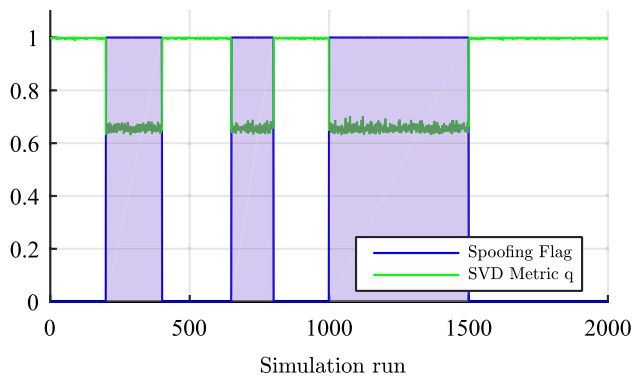


Fig. 7 Quality metric and returned spoofing flag; the noise variance was 5 degree^2 and $N = 6$

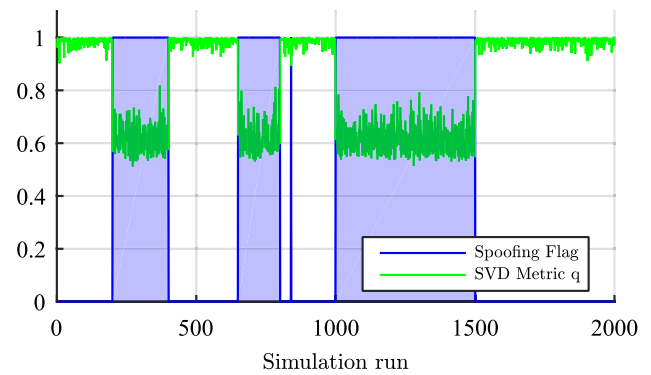


Fig. 10 Quality metric and returned spoofing flag; the noise variance was 15 degree^2 and $N = 3$

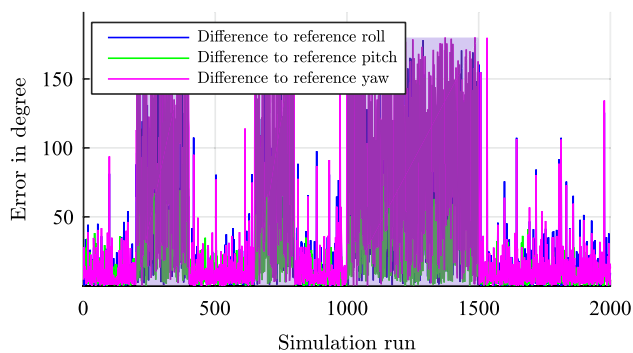


Fig. 8 Difference from reference for roll, pitch and yaw in degree; the noise variance was 15 degree^2 and $N = 3$

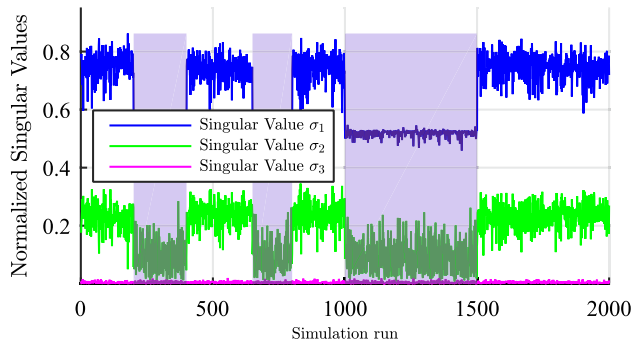


Fig. 9 Normalized singular values of C ; the noise variance was 15 degree^2 and $N = 3$

almanac measurements. The runs where a spoofer was active are indicated by a blue background.

Figure 6 depicts the resulting normalized singular values for this example.

Figure 7 shows the resulting SVD-based metric and the detection flag.

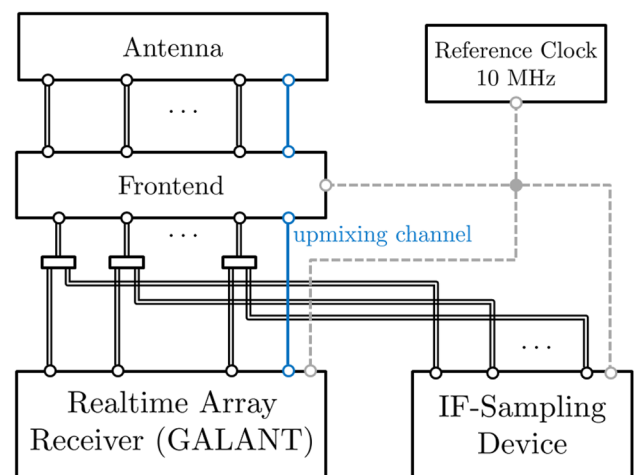


Fig. 11 Block diagram of the GNSS receiver test platform

5.2 Example 2: high noise with four signals

Again 2000 runs were performed using only 3 signals with a three times higher noise variance of 15 degree^2 . Figure 8 shows the resulting error of the attitude angles compared to the reference. The number of signals is too low to perform an estimate with such a big noise.

Figure 9 shows the corresponding singular values. When spoofing is active, the second and third singular value (σ_2 and σ_3) again almost vanish, but not completely, which is due to the noise.

As depicted in Fig. 10, spoofing detection is still almost always reliably possible. Only one mis-detection happened around epoch 800.

6 Multi-antenna GNSS receiver test platform

The detection methods shown in the previous paragraphs (Sect. 3) are implemented in a receiver platform. By using such a platform, the performance of the detection methods and algorithms can be evaluated and compared. A block diagram of the platform is depicted in Fig. 11. The following qualitative requirements are mandatory and therefore have to be taken into account during the design phase:

- Robustness against environmental conditions, i.e., salty air, is essential.
- The power consumption has to be low enough to record long enough.
- To avoid fire, the heat produced by the devices has to be acceptable.
- The downmixing has to be done for all channels synchronously in parallel.
- A calibration signal is necessary to measure and therefore compensate different latencies of the cables connecting the antennas, that are in general not equal.
- Real-time processing and recording has to be done in parallel and therefore splitting of the signal in the IF-domain is mandatory.
- All devices (i.e., mixers and AD-samplers) have to be synchronized using a common local oscillator frequency.
- The sampling rate needs to be high enough to capture the whole GPS L1 band.
- The storage (i.e., RAID-device) has to be fast and big enough to allow high bit resolutions of the sampler and several minutes of recording time.

A block diagram of the whole test equipment is depicted in Fig. 11. The details of the different parts are described in the following subsections.

An active antenna is used for reception. It includes low-noise amplifiers and RF bandpass filters. For downmixing the GPS L1 frequency band (center frequency: 1.57542 GHz) to an intermediate frequency, a front-end is used. It includes power supply for the amplifiers of the antenna, downmixers as well as a phase-locked loop frequency synthesizer, which is fed by an external 10 MHz reference. The signal is split in the IF domain. One path is fed into the sampling device. This is on custom of the shelf (COTS) hardware capable of sampling up to 16 channels in parallel. The sampled data are further processed using DLR's software receiver (MAGELLAN). The second path is fed into the real-time array receiver GALANT. Again COTS hardware is used as a basis to implement the receiver logic in both field programmable gate array (FPGA) and software. Parts requiring computational expensive operations (i.e., MACs: multiply and accumulate units) are implemented on the

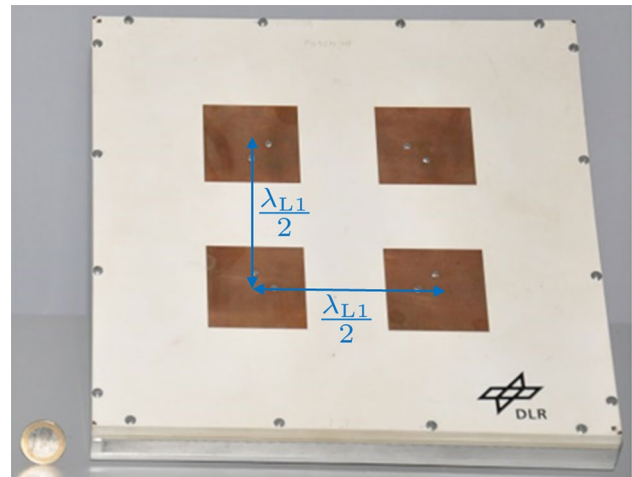


Fig. 12 Picture of the dual-band 2×2 uniform rectangular array

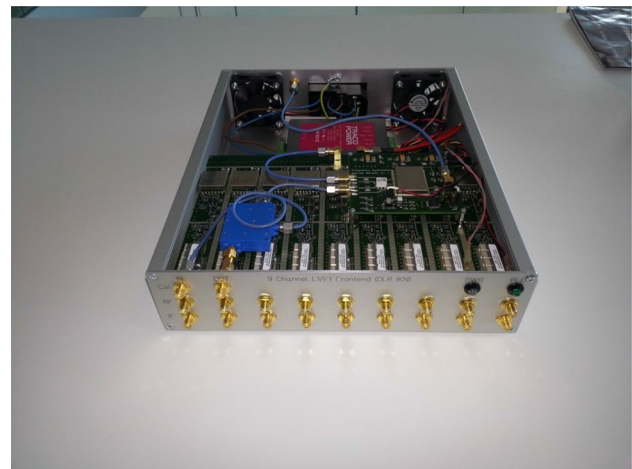


Fig. 13 Picture of the opened single-frequency RF front-end (for E1/L1), capable of downmixing up to nine channels in parallel

FPGA. Further details can be found in Refs. [32, 33]. Both the software and the real-time receiver's generic structure are depicted in Fig. 1 in Sect. 2.

6.1 Antenna array

The system's antenna is the first element of the processing chain. The 2×2 uniform rectangular array (URA) dual-frequency antenna array provides 4 degrees of freedom (DOFs). The element spacing is approximately half the wavelength for both GPS L1 and Galileo E5a. The array is depicted in Fig. 12.

The array is the key-enabler for the whole system. To enable accurate DoA estimates, a calibration input is available to inject a calibration signal (patented, see [34])

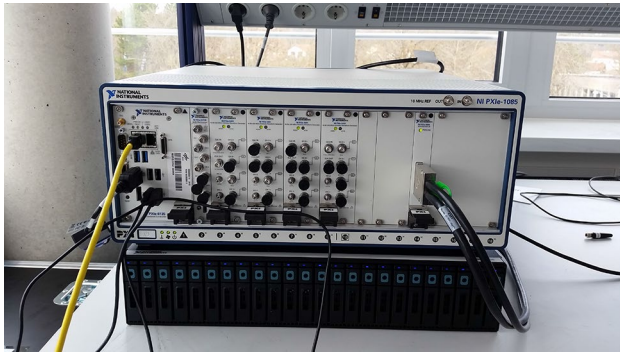


Fig. 14 Picture of the NI PXI System including the RAID storage

synchronously into all patches. The interested reader can find further details in Ref. [35].

6.2 Front-end

A single front-end (designed and manufactured by DLR) is capable of downmixing up to nine channels in parallel for a certain frequency (in that case GPS L1). The mixing is implemented following a superheterodyne principle. The frequency is derived by locking a phase-locked loop (PLL) to an external clock (10 MHz). The intermediate frequency is chosen to be 75 MHz. The signals are amplified using low-noise amplifiers (LNAs) preserving a good signal-to-noise ratio (SNR). Another key element is a highly linear phase response of the IF-bandpass filter. In parallel, one synchronous upmixing channel allows to translate the calibration signal from the IF to the HF-domain.

An opened front-end box is shown in Fig. 13.

A detailed description of the front-end design can be found in Ref. [35].

6.3 Sampling device

The sampling device is based on custom of the shelf (COTS) hardware from National Instruments (NI). The processing is customized, by modifying the software (LabView), which is executed on a NI PXIe-8135 Core i7 processor. Sampling is performed using the NI PXIe-5171R oscilloscope providing up to eight channels with a resolution of 14 bit and a sampling rate of 250 MHz. Since the available signal bandwidth of the front-end is around 20 MHz, a downsampling to 100 MHz is implemented before data storage. The operation is performed on an FPGA, which is also part of the device. This involves a bandpass undersampling mechanism. The signal's intermediate frequency after sampling therefore is 25 MHz in reverse frequency position. An external 10 MHz reference frequency is used for synchronization.

A storage device (NI HDD-8266 RAID with an overall capacity of 2 TB) is connected via an external PCIexpress



Fig. 15 Picture of the real-time receiver GALANT (including two frontends)

interface. This allows a maximum storage time of around 25 min for eight channels. The sampling device (top) and the RAID (bottom) is shown in Fig. 14.

6.4 Real-time receiver platform (GALANT)

The digital part of the real-time receiver platform is again COTS hardware (PicoDigitizer 125). The whole device is clocked, using an external 10 MHz reference frequency. 16 A/D converters have a sampling rate of 100 MHz, making the signal again visible at 25 MHz in reversed frequency position. The correlation is performed on the internal VIRTEX-6 FPGA, whereas computationally less heavy operations run on an Core i7 processor. The calibration signal is generated and transferred to the analog domain using one of the up to 8 D/A channels. This allows the calibration of different cable lengths of the reception channels.

The receiver is shown in Fig. 15 (together with an L1 and E5a front-end):

7 Experimental evaluation of the test platform

The experiments using the platform were performed in calendar week 24 of 2016. The tests including repeaters have been performed on June 17th, 2016. To be able to transmit in the GPS L1 frequency band, special permission is required. DLR is authorized by the corresponding German Authority⁸ to transmit these signals at certain locations (testbeds). For the campaign, the maritime jamming testbed in the Baltic sea (near Hiddensee) was chosen. The location is illustrated by the red circle in Fig. 16.

⁸ "Bundesnetzagentur".

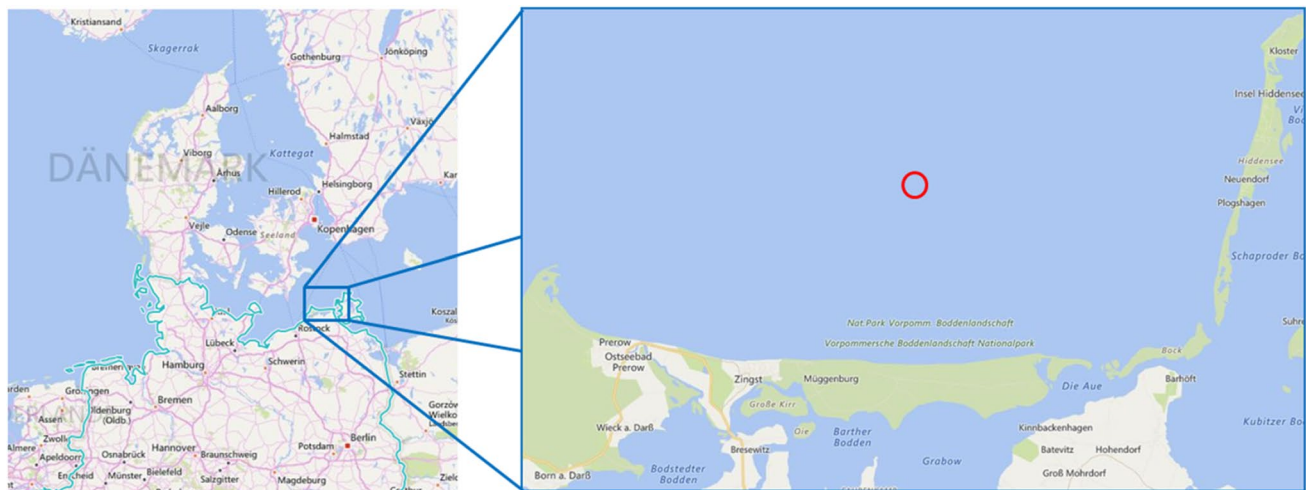


Fig. 16 Location of the jamming testbed, where the experiments have been performed

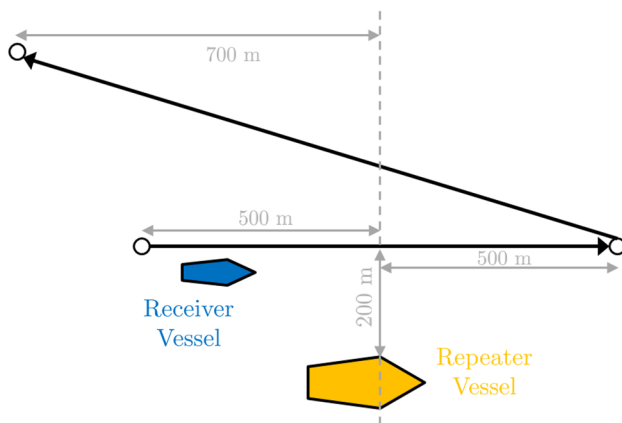


Fig. 17 Planned trajectory for the dynamic scenario

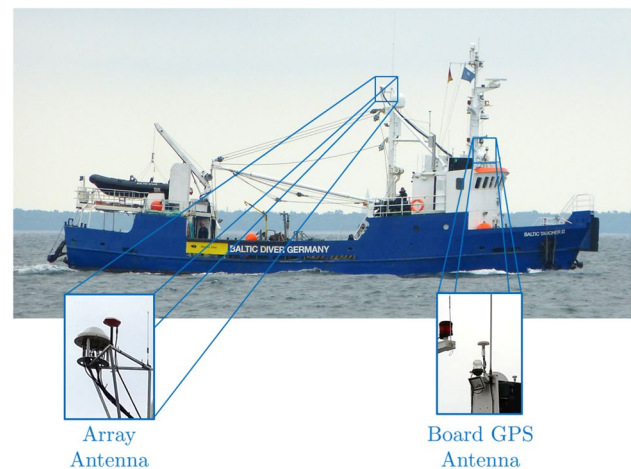


Fig. 19 Receiver vessel: the test platforms array antenna is depicted on the left and the ship's navigation system's antenna on the right

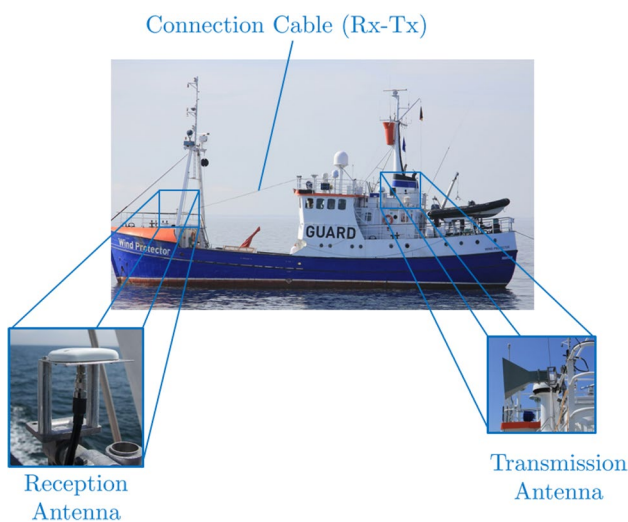


Fig. 18 Repeater installation on the transmission-vessel

7.1 Dynamic trajectory

Two ships were available to perform the experiments. The planned dynamic repeater scenario is shown in Fig. 17. The static “repeater” vessel (Wind Protector) is anchored and depicted in orange. The dynamic “receiver” vessel (Baltic Taucher II) is shown in blue.

7.2 Repeater-vessel

A picture of the repeater installation is shown in Fig. 18. An aeronautical antenna was used for reception. After conditioning of the signal (amplification), a horn antenna was installed for re-transmission. Due to export regulations, further details of the repeater setup cannot be provided.

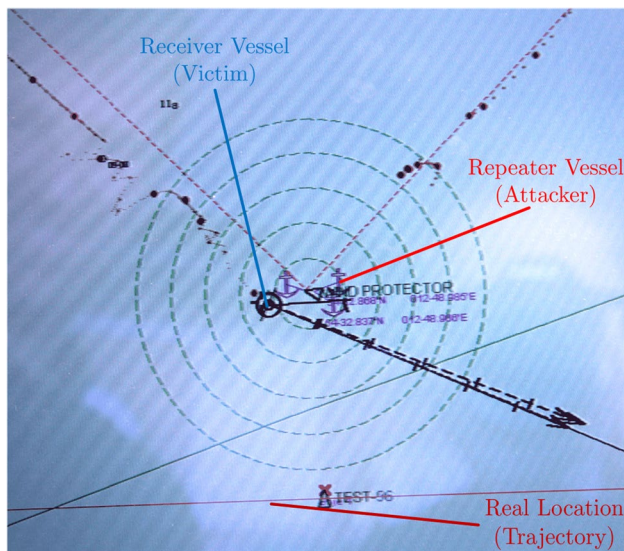
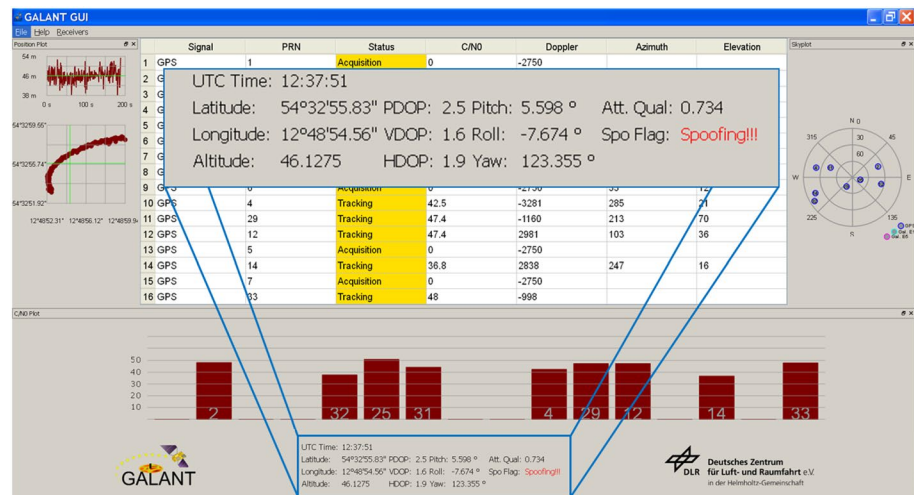


Fig. 20 Board instruments visualizing a successful repeater attack

Fig. 21 Screenshot of the graphical user interface of the GALANT receiver, indicating the presence of a spoofer/repeater



7.3 Receiver-vessel

The system described in Sect. 5 was installed on the receiver-vessel. The antennas have been mounted on the mast to avoid multipath effects caused by reflections on the metal parts of the ship. A picture is shown in Fig. 19.

7.4 Board instruments

By inspecting the board instruments, the effect on ship's navigation systems was used as an indicator for "success" of the repeater attack. An example of a successful experiment is shown in Fig. 20. The red line indicates the ground truth. During the attack, the position reported by the receiver vessel (circle) was almost the repeater vessel's one (Wind Protector, shown in green).

7.5 Real-time results

The algorithm depicted in Fig. 4 in Sect. 4 was implemented on the real-time receiver GALANT, described in Sect. 5. The processing result is sent to the graphical user interface including the "spoofing flag". In Fig. 21, the presence of a spoofer/repeater is clearly indicated.

7.6 Post-processing results

During the scenario, data were collected using the sampling device described in Sect. 5. The sampled data were fed into DLR's software receiver. The previously described attitude estimation algorithm delivers the platform's attitude together with the quality metric. A threshold of 0.985 was chosen for spoofing detection. This has been done by inspection, since not enough samples are available

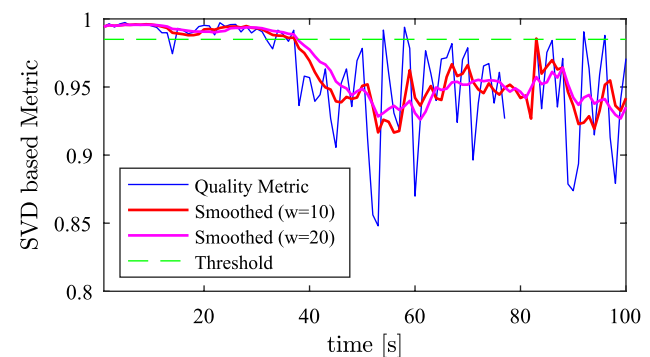


Fig. 22 Post-processing result of the attitude quality used for indicating the presence of a repeater

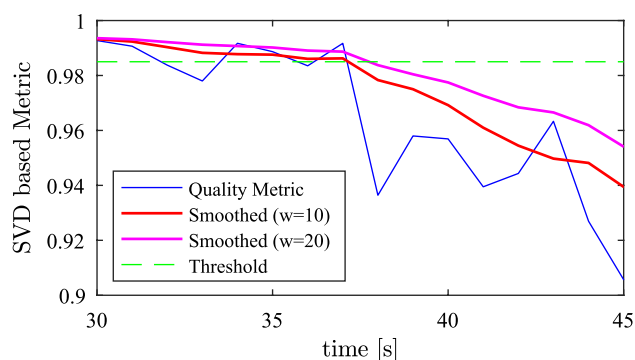


Fig. 23 Post-processing result of the attitude quality used for indicating the presence of a repeater (zoomed)

to derive and setup a clean statistical test. The result is depicted in Fig. 22.

The blue line shows the snapshot-based calculation of the singular value-based quality metric for every second. Caused by the noise added by the amplifiers of the repeater, the DoA estimates are fluctuating. Therefore, the quality metric q is fluctuating as well. This does not allow to find a proper threshold. Smoothing over a window of size w was implemented to compensate for this effect. Windows of size $w = 10$ (red line) and $w = 20$ (magenta line) are shown in Fig. 22.

A zoomed version of the plot is shown in Fig. 23. Smoothing allows for a more robust detection. The price for this is an increase in the possible time to detection of a few fractionals of a second as indicated in the plot.

For the spoofer/repeater being able to capture the receiver's tracking loops (both implementations have been parametrized similarly), the distance between the repeater and victim receiver, the amplification of the repeater as well as the noise figure of the repeater's amplifiers are the key parameters (see [36] for instance). However, once the loops are captured, the only thing that matters for detection is the estimated direction of arrival for the different impinging signals.

8 Summary and conclusion

In this work, an algorithm capable of simultaneously computing an array receiver's attitude and providing a spoofing detection was presented. The performed experimental validation was described. The algorithm is based on direction of arrival measurements from the corresponding satellites. First, by using computer simulations, the performance of the algorithm was demonstrated. The platform utilized for real-time and post-processing was introduced. Finally, an experiment using the aforementioned platform was described,

before the vulnerability of the state of the art as well the detection capabilities of the platform have been evaluated. Furthermore, the robustness of detection was increased by smoothing the returned quality metric. However, the time to detection is increased.

Acknowledgements The measurement campaign was carried out in cooperation with our colleagues from the Department for Nautical Systems. We greatly acknowledge the support, especially from Stefan Gewies, in preparing and performing the campaign. The research leading to the results in this paper is part of the project EMSEc (Echzeitdienste für die Maritime Sicherheit) and has received funding from the program Research for Civil Security of the Federal Ministry of Education and Research (BMBF) of the Federal Republic of Germany under the grant FKZ 13N12744. This support is greatly acknowledged. Special thanks goes to the most important crew member of the "Baltic Taucher II": The cook. Without the excellent food, the researches would not have been healthy enough to perform the huge amount of different experiments. Secondly, the authors would like to thank the captain of the "Baltic Taucher II". Alex's cool attitude created a relaxed and productive atmosphere.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. Allianz Global Corporate & Speciality (Hrsg.): Safety and Shipping 1912 – 2012. From Titanic to Costa Concordia. An insurer's perspective from Allianz Global Corporate & Speciality, München, London (2012)
2. Rothblum, A.: Human Error and Marine Safety Volume 4 in U.S. Coast Guard Risk-Based Decision-Making Guidelines. U.S. Coast Guard Research and Development Center, London (2006)
3. Italian Ministry of Infrastructures and Transports (Marine Casualties Investigative Body): Cruise Ship COSTA CONCORDIA, Marine casualty on January 13, 2012 (Report on the safety technical investigation), Pisa (2013)
4. International Maritime Organization, NAV 54/25 Annex 12: Strategy for the development and implementation of e-navigation, London (2008)
5. John A. Volpe National Transportation Systems Center: Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System, Cambridge (2001)
6. Grant, A., Williams, P., Ward, N., Basker, S.: GPS jamming and the impact on maritime navigation. *J. Navig.* **62**(02), 173–187 (2009)
7. Musumeci, L., Samson, J., Dovis, F.: Experimental assessment of distance measuring equipment and tactical air navigation interference on GPS L5 and Galileo E5a frequency bands. In: Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, (NAVITEC), 2012 6th ESA Workshop on, pp. 1–8 (2012)
8. Divis, D.A.: Redacted DHS report details privacy jammer risks. In: Inside GNSS, Online (2016)
9. Lloyd's Register Group Limited, QinetiQ and University of Southampton: Global Marine Technology Trends 2030, Online (August 2015)

10. European Global Navigation Satellite Systems Agency (GSA): GNSS Market Report, Online (2015)
11. Psiaki, M.L., Humphreys, T.E.: Protecting GPS from spoofers is critical to the future of navigation. In: IEEE Spectrum, Online (2016)
12. Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W., Kintner, P.M.J.: Assessing the spoofing threat: development of a portable GPS civilian spoofer. In: Proceedings of the 21st International Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, GA, pp. 2314–2325 (2008)
13. Shepard, D.P., Bhatti, J.A., Humphreys, T.E., Fansler, A.A.: Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In: Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, pp. 3591–3605 (2012)
14. Shepard, D.P., Humphreys, T.E., Fansler, A.A.: Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *Int. J. Crit. Infrastruct. Prot.* **5**(3–4), 146–153 (2012)
15. Appel, M., Hornbostel, A., Haettich, C.: Impact of meaconing and spoofing on galileo receiver performance. In: 7th ESA Workshop on Satellite Navigation Technologies NAVITEC (2014)
16. Psiaki, M.L., O'Hanlon, B.W., Bhatti, J.A., Shepard, D.P., Humphreys, T.E.: GPS spoofing detection via dual-receiver correlation of military signals. *IEEE Trans. Aerosp. Electron. Syst.* **49**(4), 2250–2267 (2013)
17. Wesson, K.D., Shepard, D.P., Bhatti, J.A., Humphreys, T.E.: An evaluation of the vestigial signal defense for civil GPS anti-spoofing. In: Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, pp. 2646–2656 (2011)
18. Broumandan, A., Jafarnia Jahromi, A., Daneshmand, S., Grard, L.: GNSS vulnerability to spoofing threats and a review of anti-spoofing techniques, Alberta Meeting, Online (Jan 2014)
19. Meurer, M., Konovaltsev, A., Cuntz, M., Httich, C.: Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM. In: Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, pp. 3007–3016 (2012)
20. Daneshmand, S., Jafarnia-Jahromi, A., Broumandon, A., Lachapelle, G.: A low-complexity GPS anti-spoofing method using a multi-antenna array. In: Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, pp. 1233–1243 (2012)
21. Konovaltsev, A., Cuntz, M., Haettich, C., Meurer, M.: Performance analysis of joint multi-antenna spoofing detection and attitude estimation. In: ION International Technical Meeting 2013 (2013)
22. Appel, M., Konovaltsev, A., Meurer, M.: Robust spoofing detection and mitigation based on direction of arrival estimation. In: Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2015), Tampa, Florida, pp. 3335–3344 (2015)
23. Meurer, M., Konovaltsev, A., Appel, M., Cuntz, M.: Direction-of-arrival assisted sequential spoofing detection and mitigation. In: Proceedings of the 2016 International Technical Meeting of The Institute of Navigation, Monterey, California, pp. 181–192 (2016)
24. Montgomery, P.Y., Humphreys, T.E., Ledvina, B.M.: Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In: Proceedings of the Institute of Navigation International Technical Meeting, Anaheim (2011)
25. Cohen, C.E.: Attitude determination. *Glob. Position. Syst. Theory Appl.* **2**, 519–538 (1996)
26. Teunissen, P., Montenbruck, O. (eds.): Springer Handbook of Global Navigation Satellite Systems. Springer, New York (2017)
27. Cuntz, M., Konovaltsev, A., Meurer, M.: Concepts, development, and validation of multiantenna GNSS receivers for resilient navigation. *Proc. IEEE* **104**(6), 1288–1301 (2016)
28. Haardt, M., Nosske, J.A.: Unitary ESPRIT: how to obtain increased estimation accuracy with a reduced computational burden. *IEEE Trans. Signal Process.* **43**(5), 1232–1242 (1995)
29. Huynh, D.Q.: Metrics for 3d rotations: comparison and analysis. *J. Math. Imaging Vis.* **35**(2), 155–164 (2009)
30. Wahba, G.: A least squares estimate of spacecraft attitude. *SIAM Rev.* **7**(3), 409 (1965)
31. Boyd, S., Vandenberghe, L.: *Convex Optimization*. Cambridge University Press, New York (2004)
32. Cuntz, M., Greda, L., Heckler, M., Konovaltsev, A., Meurer, M., Kurz, L., Kappen, G., Noll, T.: Lessons learnt: the development of a robust multi-antenna GNSS receiver. In: Proceedings of ION GNSS, pp. 21–24 (2010)
33. Kappen, G., Haettich, C., Meurer, M.: Towards a robust multi-antenna mass market GNSS receiver. In: Position location and navigation symposium (PLANS), 2012 IEEE/ION. IEEE, pp. 291–300 (2012)
34. Cuntz, M., Denks, H., Konovaltsev, A., Meurer, M.: Verfahren und empfaenger zum empfangen und verarbeiten von satellitennavigationssignalen. Patent, wO Patent App. PCT/EP2010/057,261 (2010)
35. Heckler, M., Cuntz, M., Konovaltsev, A., Greda, L., Dreher, A., Meurer, M.: Development of robust safety-of-life navigation receivers. *Microw. Theory Tech. IEEE Trans.* **59**(4), 998–1005 (2011)
36. Iliopoulos, A., Enneking, C., Jost, T., Crespillo, O.G., Appel, M., Antreich, F.: Robust ranging in the presence of repeater signals. In: Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017), Portland, Oregon, pp. 3941–3957 (2017)